UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA	**CASE NOS.: 5:18-CR-448**
Plaintiff	**JUDGE BENITA Y. PEARSON**
v.	**REPLY IN SUPPORT OF MOTION TO SUPPRESS AND MOTION TO COMPEL**
PHILIP M. POPA, JR.,	
Defendant	

Now comes the Defendant Philip M. Popa, Jr., by and through the undersigned counsel, and hereby replies in support of his previously filed Motion to Suppress and Motion to Compel. Although the Motions were filed separately, the Government opposed both Motions in one document. Therefore, for ease of use, Mr. Popa will do the same.

I. LAW AND ARGUMENT

A. POPA HAS ESTABLISHED MATERIALITY FOR HIS REQUEST TO PRODUCE THE LAW ENFORCEMENT VERSION OF FREENET

The Government argues that Mr. Popa has not established materiality in their request and that Ms. Loehrs' Affidavit is overly broad. Initially, the undersigned was candid in her initial filing that she was unaware of the issues Ms. Loehrs has addressed prior to days before the motion deadline. She had consulted with another expert and he had failed to identify any such issues. Upon learning of Ms. Loehrs and speaking with her, the undersigned felt compelled to include this in Mr. Popa's motions. There is no question that further detail and evidence of materiality would be forthcoming if Ms. Loehrs was appointed as an expert in this matter. She would review the computer seized and be able to supplement the request for the software. However, given the timing of the interaction between Ms. Loehrs and the undersigned, that was not possible. If this Court

grants his motion to appoint Ms. Loehrs, he would request to file a new or supplemental motion to compel if additional support is obtained upon Ms. Loehrs' review of the remaining evidence.

Moreover, while it is true, Freenet software is open source and publicly available, that is in fact one of the problems. Law enforcement takes open source code that is publicly available to everyone and makes very specific changes to that code for the purposes of investigation. Now that source code and program is no longer publicly available and even kept people from ensnared in their process. The Government cannot rely on the fact that Freenet is open source code that is publicly available in support of its assertions and then say what it used, which is now different, is no longer available to *anyone*. If, in fact, the open source code that is publicly available can gather the same information as the law enforcement version, there would be no need to make changes to the original.

It also appears that the Government is now saying that the Agent never claimed that Mr. Popa's IP address had child pornography. Opposition, p. 17. It appears the Government is indicating that because Mr. Popa's computer requested a small piece of a file, without knowing why or confirming he had the content, that would be enough to obtain the warrant. Instead, in order to have probable cause, law enforcement would need to demonstrate that Mr. Popa download a complete, viewable file and confirm the content is child pornography.

The Government also claims that Ms. Loehrs "repeatedly trashes law enforcement tools" and has been repeatedly denied the ability to review software. The Opposition also faults her for failing to include the results of prior reviews. Ms. Loehrs has been repeatedly permitted to review law enforcement software. Her extensive CV was attached to the Motion requesting her appointment. The most recent court to allow her to review the software issued was US v. Anthony Espinoza Gonzales, No. CR-17-01311-001-PHX-DGC, United States District Court for the

District of Arizona. In that case and others, Courts have found that a review of the software used by the Government is necessary to allow the Defendant to effectively defend himself. It is especially important in this matter where the Government admits that their Affidavit in support of the search warrant contains no direct evidence that Mr. Popa's computer ever received or requested a full file of child pornography. Further, Ms. Loehrs is not permitted to ever discuss what she locates when she reviews law enforcement software. When she is permitted access, she is covered by a protection order that does not allow disclosure.

Finally, as it relates to Ms. Loehrs, the Government claims that she is traipsing through the country making fantastic claims to further her business. She has worked on over 1,000 cases all over the world, including 500 cases involving child pornography. The issues raised in her affidavit have only been presented in approximately 60 cases. An affidavit indicating this has been requested and will be filed upon receipt.

B. THE LAW ENFORCEMENT SURVEILLANCE SOFTWARE IS PROTECTED BY QUALIFIED PRIVILEGE AND SHOULD NOT BE PRODUCED IN DISCOVERY

The Government lists various concerns regarding the disclosure of the software. Each and every one of those concerns is adequately addressed with a protective order. As noted above, Ms. Loehrs has been provided access to a variety of law enforcement tools. When that occurs, she is subject to a protective order and is unable to relay what she learns to anyone not involved in the particular case. This is not uncommon in a variety of federal criminal investigations. For example, the same precautions are taken when the Government is pursuing allegations of terrorism or even ongoing public corruption. The individuals involved must be subject to a protective order protecting them from divulging information they receive in the course of their work on the case.

There is no reason that same procedure would not be effective here in addressing the Government's concerns.

C. MR. POPA'S IP ADDRESS WAS IMPROPERLY OBTAINED BY AN ADMINISTRATIVE SUBPOENA.

The Government claims that Mr. Popa has attempted to incorrectly expand the holding in Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed2d 507 (2018). While the Government is correct that Carpenter dealt with location information, the holding upended the prior precedent that individuals have no reasonable expectation of privacy in information held by a third party. This has been an ongoing development of the digital error and the Supreme Court in United States v. Jones, 132 S. Ct. 945, 957 (2012) noted that the third party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." Five Justices have "expressed the view that technology has changed the constitutional calculus by dramatically increasing the amount and precision of data that the government can easily collect." Jones, 132 S. Ct. at 955-56 (Sotomajor, J., concurring); 964 (Alito, J., concurring).

Post-Carpenter, Courts must reevaluate the third-party doctrine's application to the digital world. The Government claims that information such as an address or phone number of an internet subscriber is not the type of information at issue in Carpenter. However, this ignores the essentially unique aspect of internet traffic and access to a person's private data. As the Supreme Court noted, people reveal a great deal about themselves online. For example, an individual may seek to learn about HIV because they have been recently diagnosed. That information is anonymous until the identity of the IP address holder is exposed. Therefore, the information at issues with an administrative subpoena is not simply a person's address, it is the connection between that address and their history in the digital world. Moreover, the IP address changes according to who is providing the internet service, including a coffee shop, home router, the department store, and doctor's

office. So, similar to the information in Carpenter, the IP address may reveal an individual's movements in society. When that traffic in the digital or physical movement evidences illegal conduct, a warrant may be obtained to receive the information sought. An administrative subpoena does not provide the necessary protection after the Supreme Court ruled in Carpenter that individuals have a reasonable expectation of privacy in information held by a third party.

D. THE SEARCH WARRANT WAS NOT SUPPORTED BY PROBABLE CAUSE AND THE GOOD FAITH EXCEPTION DOES NOT APPLY

The Government's Opposition claims that Mr. Popa focuses his entire attack of the search warrant affidavit on the reliability of the law enforcement program and the mathematical formula it relies upon. This is not entirely incorrect as much of the affidavit is background information not having anything to do with the specific IP address at issue. The Affidavit also makes it clear that it is only through the program and mathematical formula that it can be alleged that the IP address at issue is actually even interacting with child pornography.

The basis for the Affiant's statement that the mathematical formula in the article is accurate is the fact that it was peer-reviewed. The Government claims that there is evidence of this in the article itself. In fact, what is contained in the article is "© 2017 Copyright held by the authors. From Proc. IEEE International Workshop on Privacy Engineering, May 2017." Neither of these indicates that the article was in fact peer-reviewed. It certainly does not provide any information that the Affiant believed it to be a peer-reviewed article. Moreover, Exhibit A does not demonstrate that the article was peer-reviewed as that term is understood to ensure reliability.

WHEREFORE, Defendant Popa, hereby respectfully requests that this Honorable Court grant his prior motions.

Respectfully submitted,
WILLIAM T. WHITAKER CO. LPA

/s/Andrea Whitaker
ANDREA WHITAKER #0074461
54 E. Mill Street Suite 301
Akron, Ohio 44308
T: 330-762-0287 F: 330-762-2669
whitaker@whitakerlawlpa.com
Attorney for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was electronically filed this 22nd day of February, 2019. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system.

/s/ Andrea Whitaker
Andrea Whitaker